17352

Emanate Health

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

Re: Notice of Data Breach

Emanate Health (formerly Citrus Valley Health Partners) values the relationship we have with our current and former employees and understands the importance of protecting personal information. We are writing to inform you about a data breach involving one of our third-party vendors, PaperlessPay Corporation ("PaperlessPay"), that involves your personal information. PaperlessPay is a payroll processing company that we have contracted with to process and deliver electronic pay stubs and W-2 tax forms. This notice explains the incident, the measures that have been taken, and some steps you can take in response.

What Happened? We received notice from PaperlessPay on March 20, 2020 informing us that an unauthorized person gained access to its computer server. PaperlessPay learned of the incident on February 19, 2020 when the Department of Homeland Security ("DHS") contacted PaperlessPay to inform them that an unknown person was purporting to sell "access" to the PaperlessPay database on the dark Web.

In response, PaperlessPay shut down its web server and Structured Query Language ("SQL") server to prevent any potential unauthorized access. The server shutdown prevented you from accessing payroll records online for a period of time while the servers were offline. Over the following weeks, PaperlessPay cooperated with a joint investigation conducted by DHS and the Federal Bureau of Investigation ("FBI"), and PaperlessPay retained a cybersecurity firm to help with its internal forensic investigation of the incident.

The investigations confirmed that an unknown individual accessed PaperlessPay's SQL server where employee data is stored on February 18, 2020. The available evidence has not, however, allowed DHS, the FBI, or PaperlessPay's cybersecurity firm to determine what data the individual may have accessed or viewed while connected to the SQL server. It is possible the person only used the access to determine the size of the SQL database and to stage it for subsequent access that could be sold to others, and that the individual did not directly access any employee data. However, the individual would have had the capability to run queries against the SQL database and view its data, so PaperlessPay cannot rule out the possibility of unauthorized access or acquisition of your personal information.

What Information Was Involved? The information stored in the SQL server about employees consists of the data components that appear on their pay stubs and tax forms, including their name, address, pay and withholdings, last four digits of bank account number (if that information is included on the pay stubs), and Social Security number. These data components are stored on the SQL server in different tables that are associated by user ID numbers, not names, within each table. Therefore, the only way to associate any data with an individual would be to run a query against the database and have it aggregate an individual's name with his or her other data components. PaperlessPay could not conclusively determine whether such queries were run. *No bank account passwords or access codes were stored on the SQL server.*

What Is PaperlessPay Doing? PaperlessPay has indicated that it has acted to secure its network and prevent future incidents. In order to resume its services, PaperlessPay has rebuilt an entirely new domain controller, a new web server, and a new SQL server. PaperlessPay has also indicated that it then restored database files to the new SQL server from backups, assigned new IP addresses to all of the new servers, changed all passwords for users and administrators, implemented a setting that requires clients to change their passwords when they login for the first time, and disabled all remote access capabilities to the new web server and SQL server. PaperlessPay further reported that it installed an endpoint detection and response application on the new servers and other endpoints within its network that has enabled PaperlessPay to monitor all activity while PaperlessPay completed its investigation of the incident.

For Emanate Health's part, we have been working with PaperlessPay to obtain details of the incident and the affected accounts and to obtain assurances that information about our employees is safe. In order to provide you with information you can use to better protect against identity theft and fraud, Emanate Health is offering free credit monitoring services for 24 months. Instructions for enrolling in the credit monitoring services, as well as additional information on how to better protect against identity theft and fraud, are included in the attached Privacy Safeguards and last page of this letter.

What Can You Do? You should review and follow the attached Privacy Safeguards for how to protect against identity theft and fraud. You can enroll to receive the free credit monitoring services by following the instructions listed on the last page of this letter.

For More Information. We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please call our toll-free assistance line at 855-907-2124, Monday through Friday, from 6 am to 6 pm PST. We regret that this incident occurred and apologize for any concern or inconvenience this may cause you.

Sincerely,

R. Eric Maristela
Corporate Compliance & Privacy Officer

PRIVACY SAFEGUARDS

Enroll in Free Credit Monitoring. As an added precaution, we encourage you to sign up for credit monitoring services for 24 months at no cost to you. These services are provided by TransUnion. Please see the included credit monitoring information at the end of this letter.

Monitor Your Account Statements. We also encourage you to remain vigilant against incidents of identity and fraud, and to review your credit and bank account statements for suspicious activity. You should promptly report suspected identity theft to appropriate authorities.

Request Your Credit Reports. You are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. When you receive your credit reports, read them carefully. Look for accounts you don't recognize. Look in the inquiries section for names of creditors from whom you haven't requested credit. If you find anything you don't understand, call the credit bureau at the telephone number listed on the report.

Consider Placing a Fraud Alert on Your Credit File. You can place an initial or extended "fraud alert" on you file at no cost. An initial fraud alert is a 1-year alert that is placed on your credit file. Upon seeing a fraud alert display on your credit file, a business is required to take steps to verify your identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	TransUnion P.O. Box 105069 Chester, PA 19016 1-800-909-8872 www.transunion.com	Equifax P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.alerts.equifax.com

Consider Placing a Security Freeze on Your Credit File. You also have the right to place a "security freeze" on your credit file, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make for a new loan or extension of credit. You cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed above, or use the following links:

Experian: www.experian.com/freeze/center.html
TransUnion: www.transunion.com/credit-freeze
Equifax: https://www.equifax.com/personal/credit-report-services/credit-freeze/

For More Information. You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338). The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. To file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be promptly reported to law enforcement and your state Attorney General.

TransUnion

Activation Code: <<Activation Code>>

Complimentary 24-Month *my*TrueIdentity Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for 24 months provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery.

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)